Recent Developments in Covert Acoustical Communications

Michael Hanspach and Michael Goetz
Fraunhofer FKIE, Wachtberg, Germany
{michael.hanspach, michael.goetz}@fkie.fraunhofer.de

Abstract: The topic of covert acoustical communication in air has produced public attention, lately. In 2013, we presented the fact that infected drones (e.g. laptops) might form covert acoustical mesh networks in air, only utilizing the built-in speakers and microphones. In this article, we aim to present the current state of covert acoustical communication in air. We discuss future forms of covert acoustical mesh networks, we present an alternative audio signal that is improved in terms of stealthiness, and we provide considerations on the stealthiness of covert acoustical communication in air. In order to protect computing setups from malware utilizing covert acoustical communications, we present an analysis on detection and localization mechanisms for covert acoustical transmissions. Finally, we describe the implementation of an audio intrusion detection system that is designed for automatic analysis of acoustical emanations.

1 Introduction

Covert acoustical communication in air is a serious threat to computer security as identified by Hanspach, Keller and Goetz [HK13b, HK13a, HG13], as it may circumvent operating system and network security policies, unless this type of attack is considered in the security design of the computing system's components.

In November 2013, we finally published the concept and implementation of a covert acoustical mesh network in air [HG13]. Reutilizing the Adaptive Communication System (ACS) (see also [ON10, NG12, GN12, MTZ10]) that has originally been developed for robust acoustic underwater communication by the Research Department for Underwater Acoustics and Marine Geophysics (FWG) of the Bundeswehr Technical Center WTD 71, Kiel, Germany, a robust low-bandwidth communication scheme for air-based wireless mesh networks was discussed. Following the presented approach, future malware might utilize covert acoustical communications to even extract information from computers that are not connected to any regular type of network (e.g. Ethernet or WLAN). Our work on covert acoustical mesh networks has been widely covered by public media (e.g. [Goo13, Owa13, Com13]).

Further research on these covert networks is important, as current security policies might be easily circumvented by covert communications. This threat is even intensified by the

Corresponding author email: michael.hanspach@fkie.fraunhofer.de

fact that some devices (e.g. smartphones) are not shipped without speakers and microphones, and a mobile phone without microphones and speakers would be useless in regard to its original purpose (i.e. phone conversations).

In the terminology of this article, the term *covert* refers to the fact that we are using means for communication that have not been designed for computer-to-computer communication at all (i.e. acoustic wave propagation with built-in audio devices). Because of this, the presented acoustical channel can be described as a *covert channel* [Lam73]. Applying the definition of a covert channel to the context of computing systems separated by air gaps [IET07], we define a **covert network** as:

A network that exists independently from established types of network interfaces and utilizes physical means for computer-to-computer communication that have not been designed for this type of communication.

In difference to this *covertness*, the term *stealthiness* refers to the fact that we hide the very presence of communication from detection of human computer users. Stealthiness is *not* an absolute property. Instead, different degrees of stealthiness can be conceived as distinct points of a stealthiness continuum. Increasing the degree of stealthiness of a covert network is only possible to a certain degree and can sometimes come with drawbacks regarding the impact of the covert network (e.g. reducing the maximum range per hop as described in Section 2).

Our contribution to the field includes the presentation of an alternative audio signal, considerations on the stealthiness of a covert acoustical malware, the presentation of detection and localization mechanisms for covert acoustical communications, and the implementation of an audio intrusion detection system.

The remainder of this article is structured as follows. Details on the implementation and evaluation of an alternative audio signal within the ultrasonic frequency range and further considerations on stealthiness are provided in Section 2. In Section 3, we present methods for detecting covert acoustical communications in the presented form. In Section 4, we present the implementation of an adaptive audio intrusion detection system. In Section 5, we briefly discuss related work and how it differs from our work. In Section 6, we conclude the article.

2 Advances in covert acoustical communications

2.1 Implementation and evaluation of an alternative signal that is placed within the ultrasonic frequency range

To demonstrate the high transmission range per hop achievable (19.7 m) within this covert network, the audio transmissions generated in the first experiment on covert acoustical communications [HG13] have been placed into the near ultrasonic frequency range $<$ 20,000 Hz. Although the sound processor of commonly available computers (i.e. Lenovo T400 laptops) gradually attenuates the ultrasonic frequency range between 20,000 Hz and

25,000 Hz [HG13], audio transmissions might also be placed into a narrow band of the available ultrasonic frequency range $\geq$ 20,000 Hz in order to prevent any chance of human detection (even at high volume levels). However, as an acoustical malware would be in control of the volume levels of any modem transmission, and might adapt to the configured system volume levels, the original signal already delivers a relatively high degree of stealthiness and might not be detected easily.

The remainder of this section includes an alternative approach where the audio signal of the ACS modem is put entirely into the ultrasonic frequency range. The alternative audio signal implements FHSS (frequency hopping spread spectrum) with 20 carriers, providing an ultrasonic frequency range from 20,500 to 21,500 Hz that may fit just right into the available ultrasonic frequency range of the utilized sound processor. The bit rate of approximately 20 bit/s and the latency of 6 s per hop remain unchanged with this frequency shift. Although the delivered bandwidth is not comparable to the capabilities of the established wireless communication standards, it is actually high enough to transfer small portions of critical data such as keystrokes from the keyboard of a human computer user, private encryption keys and malicious command-and-control data [HG13].

Moreover, much higher transmission rates are achievable at a closer distance, as we will show in a future article.

While humans walking through the experiment setup are found to be interfering with the transmissions, this effect does not defeat the effectiveness of the covert network at all, as GUWMANET/GUWAL transmissions without a received acknowledgment are simply retransmitted [GN12]. The frequency range of the alternative audio signal is shown in Fig. 1.

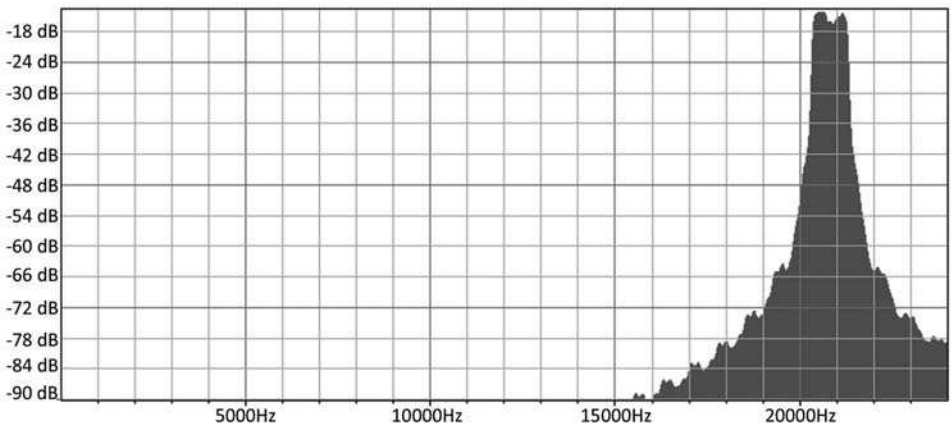

Figure 1: Frequency range (before filtering) of the alternative signal with the ACS modem (FFT, size 1024, Hanning window)

As can be seen in Fig. 1, the frequency range has been completely moved into the ultrasonic frequency range $\geq$ 20,000 Hz at relative volume levels between -12 dB and -48 dB. The spectrogram of the alternative audio signal is shown in Fig. 2.

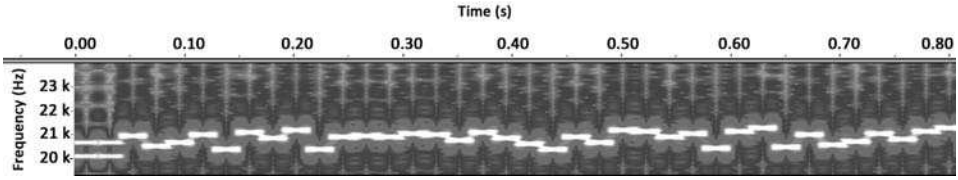

Figure 2: Spectrogram (before filtering) of the alternative signal with the ACS modem

The waveform (Fig. 3) was adapted in order to prevent intersymbol interference by application of a trapezoid window and the square root of a Hamming window defined by: $\sqrt{0.54 + 0.46 \cdot \cos\left(\frac{2\pi(i-1024/2)}{1024}\right)}$ for each index i. These measures have shown to produce less acoustic energy in the surrounding frequencies.

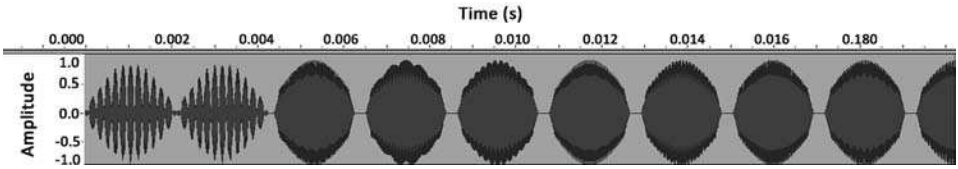

Figure 3: The adapted waveform (windows applied)

To support audio transmissions with the alternative signal, and to increase the stealthiness at high volume levels, a newly adapted bandpass FIR filter (Fig. 4) is utilized for the main part of the signal.

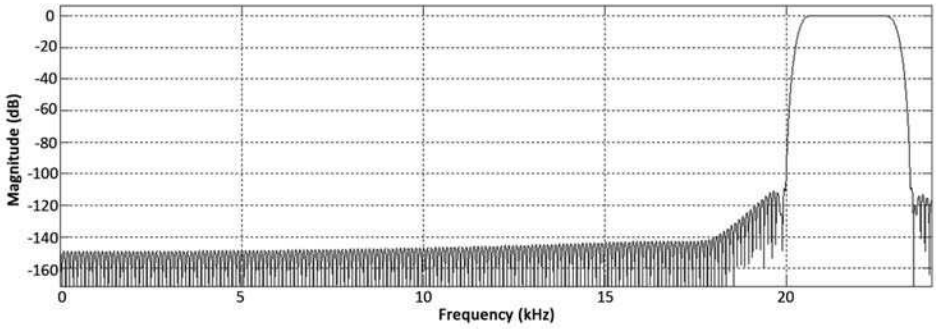

Figure 4: The newly designed bandpass FIR filter (Blackman-Harris window, 20.4 kHz - 23.0 kHz)

In order to prevent potentially audible artifacts of the signal, the bandpass FIR filter is installed both at the receiver and the transmitter. Because of the audio filtering, it is even possible to play mp3 files at the same time as transmitting data.

2.2 Range Experiment

The range experiment (see also [HG13]) is rerun in order to determine the maximum range achievable per hop. The range experiment is described in the following. Two isolated computing systems (type: Lenovo T400) are placed in an approximately 25 m long corridor. The laptop covers are opened and the laptop audio input and output devices are loosely directed at each other. No acoustical preparations are made in the course of the experiment setup. The maximum transmission range between 2 nodes is determined by sending out messages, and by measuring and gradually increasing the transmission range between the nodes with each successful transmission.

As a result of the range experiment, it was determined that a maximum range of 8.2 m per hop can be achieved with the alternative signal (19.7 m with the originally presented signal). Therefore, a potential attacker would have to choose between maximum stealthiness and maximum communication range in the design of a malware.

Further tests with a prerecorded and replayed audio transmission suggest that other types of devices (i.e. smartphones) are, in fact, able to communicate at a comparable distance.

2.3 Considerations on stealthiness

With the alternative signal, a *covert network* might be *stealthy* in the following meanings:

1. A covert network might be *stealthy* by running the communication system as a background process on the computing system and might implement advanced process hiding mechanisms (see also [Ger04, Flo05]).
2. A covert network might be operating in a very *stealthy* state, i.e. only occasionally sending out important data such as gathered passwords and encryption keys.
3. A covert network might be *stealthy* in terms of preventing human detection at high volume levels by solely utilizing the ultrasonic frequency range.
4. A covert network might also be *stealthy* by steganographically hiding the transmission in the background noise (e.g. as already proposed for underwater networks [LvW08]). However, this might not be practical in air-based networks, where much smaller distances are overcome in comparison to underwater networks. Because of this, the user might be able to locate and, therefore, detect the transmissions (e.g. ventilation fan noise that is apparently produced by the speakers).

As the presented approach for a covert network does not feature steganography, computer-aided identification of the communications is feasible as shown in the following section.

3 Considerations on the detection and localization of covert audio transmissions

3.1 Audio profile of an unmodified laptop computer

Covert acoustical communications can be visualized with the help of a spectrum analyzer that produces a pattern similar to the pattern shown in Fig. 2. However, detection of covert acoustical communications from looking at a spectrogram can be a non-trivial task as other audio sources within the computing system are present that might be erroneously interpreted as a covert audio transmission. This fact is presented in Fig 5, where the audio profile of a laptop (type: Lenovo X201) is analyzed (without any covert communications).

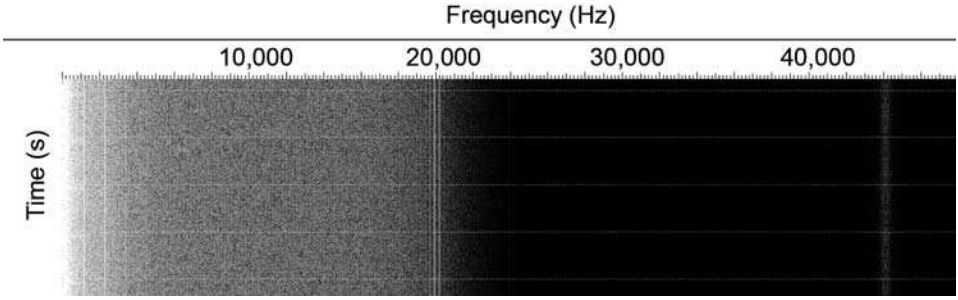

Figure 5: Spectrogram of sounds emitted by an unmodified laptop

The spectrogram was recorded with an external microphone (AKG C 1000 S) at a distance of 20 cm between the microphone and the laptops's ventilation opening. Although the microphone is primarily designed for recordings $\leq$ 20,000 Hz, it is also capable of recording some parts of the ultrasonic frequency range according to the manufacturer's specification [AKG]. The analysis reveals the presence of acoustical emanations that form a narrow band around 20,000 Hz and are apparently generated by the laptop's ventilation fan. Thus, the presence of ultrasonic emanations from unmodified laptops has to be considered in visual analyses. As LeMay and Tan [LT06] supposed, there might be further interesting emanations in the ultrasonic frequency range. However, as the sound processor of common laptops (i.e. Lenovo T400 and T410 types) gradually attenuates signals between 20,000 and 25,000 Hz [HG13], communication with the internal speakers and microphones can only occur in the frequency range below 25,000 Hz.

3.2 Experiment on detection and localization of covert audio transmissions

As an early warning system against covert acoustical communications, a frequency converter can be utilized to pitch down inaudible frequencies and produce an audible signal with each transmission. In a combined experiment on visual and acoustical detection of covert acoustical communications, we utilize the Rohde & Schwarz PR100 portable re-

ceiver that was originally designed for on-site radio monitoring [Roh]. Over a specially crafted connector, the PR100 is electrically connected with a microphone as its input device and configured to capture the frequency range around 20,000 Hz. A laptop is configured to output covert audio transmissions. The internal display of the PR100 is used for the visual detection mechanism (spectrum analyzer) and the internal speakers of the PR100 are used as output devices, while converting the recorded audio input back to humanly audible frequencies around 2,000 Hz. With comparable devices, detection of covert acoustical communications can be implemented as a mobile or stationary service. The same approach might also be implemented in software. The described detection and localization experiment is depicted in Fig. 6.

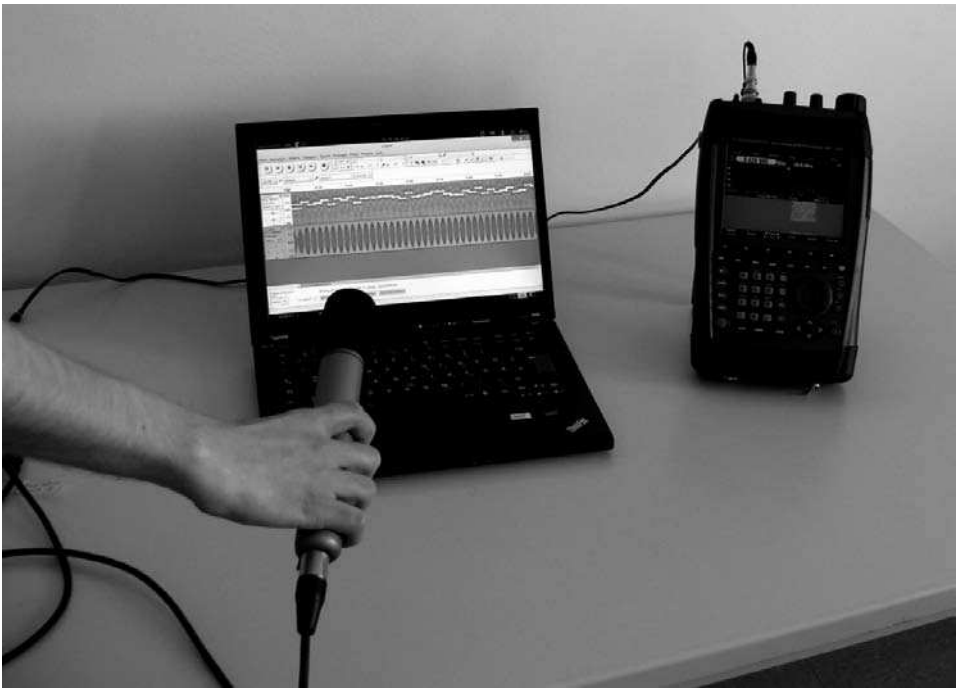

Figure 6: Locating the source of a covert audio signal with a mobile device (PR100)

As a result of the detection and localization experiment, the acoustical detection mechanism produces a specific audio output that is characteristic to the utilized frequency hopping sequence used in our experiments and, therefore, offers an easy-to-implement solution to detect this specific type of audio signal. The audio source could be exactly located by pointing the microphone in different directions and following the path of the loudest audio output. However, the acoustical detection mechanisms might also suffer from previously inaudible audio sources that could erroneously appear as an audio signal. Therefore, these detection mechanisms are most applicable if the characteristics (i.e. the signature, as explained in the following section) of the audio signal are previously known.

Moreover, if a highly advanced type of malware would hide acoustical communications in

a low signal-to-noise ratio (e.g. as shown in underwater networks [LvW08, vWLS+09]), the detection mechanisms presented so far might not be successful. In difference to underwater networks, we suppose this technique only to be feasible for ultrasonic sources of noise, as a speaker emitting background noise (e.g. the audible parts of the typical fan noise) could immediately attract the user's attention.

Finally, data transmissions might also be steganographically hidden within audible sound playback [PK00], but this would limit communications over the covert network to situations where audio playback is actually initiated by the user.

Detection of these types of audio signals can also be automated for use in an audio IDS (intrusion detection system) as described in the following section.

4 Implementation of an adaptive audio intrusion detection system

Based on a previously patented signal detection and autocorrelation method for radio communications [KLP12], we describe the implementation of an adaptive audio IDS. The underlying framework operates along the following principles:

1. A time slice of a prerecorded signal is extracted and analyzed.
2. Different signal characteristics are extracted from the signal for further analysis.
3. The captured signal characteristics are stored as a signature of a known signal.
4. During the operation of the audio IDS, live captured signal data is matched against the stored signatures.
5. Upon a match, an intrusion warning regarding the detection of a known audio signal is generated.

In our demonstration, an extracted time slice of approximately 2.5 seconds is selected from a covert audio transmission (see Fig. 7).

For automatic intrusion detection of the presented signal, the frequency shift utilized in the previously depicted frequency hopping sequence was found to be a suitable characteristic for automatic signal detection. Fig. 8 shows the results of the frequency shift analysis.

As can be seen in Fig. 8 the frequency shift analysis reveals a peak at 45.8 Hz, which matches the most prevalent frequency shift between two modulated audio tones. Moreover, local peaks at 91.6 Hz and other multiples of 45.8 are shown in Fig. 8. The observed frequency shift thus offers a reliable characteristic for the automatic detection of the presented audio signal and for related audio signals.

Alongside the frequency shift analysis, different methods and characteristics might be utilized for signature generation and matching (e.g. CA-CFAR, see also [Gie12]), as well as periodicity and structure repetition [Kur13]).

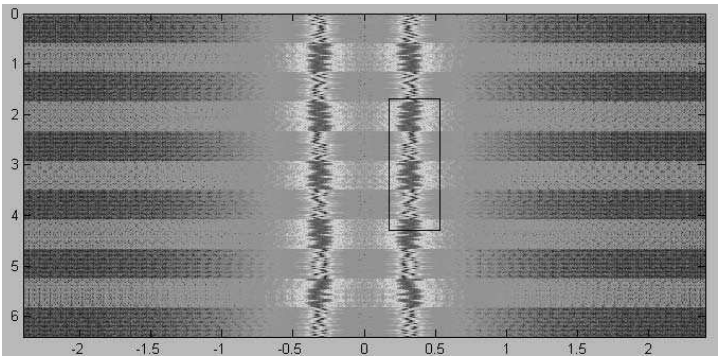

Figure 7: Time slice extracted from the recorded audio input

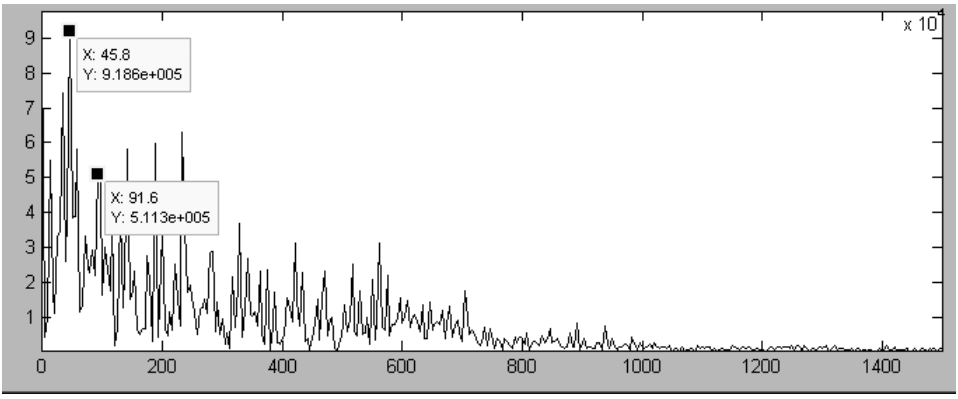

Figure 8: Automatically detecting covert audio signals by frequency shift analysis

The audio IDS is designed as an *adaptive* framework, as various signal characteristics can be chosen as detection patterns and new types of audio signals can easily be integrated into the framework. As we previously suggested, the audio IDS might be implemented within a trusted operating system component (i.e. as an audio intrusion detection guard [HG13]).

5 Related work

Acoustical networking has been suggested by several authors [MSTS05, NCPV13] and preliminary studies on ultrasonic communication in a very different context have been conducted [TOD+10, HSH+13]. Moreover, acoustical communication is commonly used in underwater networks [OAC+12]. In difference to these authors, we put covert acoustical communications and acoustical mesh networks (e.g. as present in underwater networks) into the context of operating system security [HK13b, HK13a], and covert networks [HG13], respectively. Additionally, we present the current state of covert networks.

6 Conclusion

We have discussed recent developments in air-based covert acoustical communications.

An alternative signal for the previously described ACS modem has been presented that operates solely in the ultrasound frequency range, although the maximum transmission range was found to decrease with common laptops. Still, the impact of the covert network might be greatly extended by the regular movements of these mobile devices. A new bandpass filter was presented with the intention to filter out potentially audible acoustical artifacts. The stealthiness of the original signal has been improved, but steganographic methods may additionally be applied to also hide the signal from visual and acoustical detection mechanisms as presented here.

Various techniques for the detection and localization of covert acoustical communication have been discussed and the implementation of an adaptive audio intrusion detection system has been presented. It was demonstrated that automatic detection of covert acoustical communications is feasible by comparing the characteristics of the live recorded emanations with the previously stored signatures of audio signals.

While covert networks might also be implemented over malicious hardware, we conclude that the software-based approach is much more feasible, as infection can occur over traditional means (e.g. over removable media, and over the internet, if the computer is temporary connected to the internet), and does not rely on tampering the supply chain for the purchase of new computers.

In summary, covert networks might arise as an upcoming trend in future malware and have to be considered in the design and implementation of future security critical computing systems.

Acknowledgment

We would like to thank Jörg Keller for helpful comments and Ivor Nissen for making this research possible. Special thanks goes to Frank Kurth for helpful information on signal detection methods. We further acknowledge Hans-Peter Stuch and Christian Schlich for helpful assistance regarding the detection and localization experiment.

References

[AKG] AKG. AKG C 1000 S Condenser Microphone. http://www.fullcompass.com/common/files/2186-akg_c1000s_specs.pdf, Accessed: 2013-12-01.

[Com13] Communications of the ACM. Experimental Malware Uses Inaudible Sound to Defeat Network Air Gaps. http://cacm.acm.org/news/170320-experimental-malware-uses-inaudible-sound-to-defeat-network-air-gaps/fulltext, Accessed: 2013-12-05, December 2013.

[Flo05] Elia Florio. When Malware Meets Rootkits. *Virus Bulletin*, 2005(12), December 2005.

[Ger04] Gergely Erdélyi. Hide'n'Seek? Anatomy of Stealth Malware. http://download.adamas.ai/dlbase/ebooks/VX_related/Hide%27n%27Seek%20Anatomy%20of%20Stealth%20Malware.pdf, Accessed: 2013-12-01, March 2004.

[Gie12] Ryan Thomas Gieleghem. Robust Acoustic Signal Detection and Synchronization in a Time Varying Ocean Environment. Master's thesis, Massachusetts institute of Technology, October 2012.

[GN12] Michael Goetz and Ivor Nissen. GUWMANET - Multicast Routing in Underwater Acoustic Networks. In *Military Communications and Information Systems Conference*, MCC '12, pages 1–8. IEEE, October 2012.

[Goo13] Dan Goodin. Scientist-developed malware prototype covertly jumps air gaps using inaudible sound. http://arstechnica.com/security/2013/12/scientist-developed-malware-covertly-jumps-air-gaps-using-inaudible-sound/, Accessed: 2013-12-02, December 2013.

[HG13] Michael Hanspach and Michael Goetz. On Covert Acoustical Mesh Networks in Air. *Journal of Communications*, 8(11):758–767, November 2013.

[HK13a] Michael Hanspach and Jörg Keller. A Taxonomy for Attack Patterns on Information Flows in Component-Based Operating Systems. In *Proceedings of the 7th Layered Assurance Workshop*, New Orleans, LA, USA, December 2013.

[HK13b] Michael Hanspach and Jörg Keller. In Guards we trust: Security and Privacy in Operating Systems revisited. In *Proceedings of the 5th ASE/IEEE International Conference on Information Privacy, Security, Risk and Trust*, PASSAT '13, Washington, DC, USA, September 2013. IEEE.

[HSH+13] Ragib Hasan, Nitesh Saxena, Tzipora Haleviz, Shams Zawoad, and Dustin Rinehart. Sensing-enabled channels for hard-to-detect command and control of mobile devices. In *Proc. 8th ACM SIGSAC symposium on Information, computer and communications security*, ASIA CCS '13, pages 469–480, New York, NY, USA, 2013. ACM.

[IET07] IETF Network Working Group. RFC 4949. Internet Security Glossary, Version 2. http://tools.ietf.org/html/rfc4949, Accessed: 2013-12-16, August 2007.

[KLP12] Frank Kurth, Hans Günter Lehn, and Rolf Parting. Patent DE102009035524 B4. Verfahren zur Erkennung eines oder mehrerer Nutzsignale innerhalb eines Quellsignals (German language content). http://www.google.com/patents/DE102009035524B4?cl=de, Accessed: 2013-01-29, November 2012.

[Kur13] Frank Kurth. The shift-ACF: Detecting multiply repeated signal components. In *IEEE Workshop on Applications of Signal Processing to Audio and Acoustics*. IEEE, October 2013.

[Lam73] Butler W. Lampson. A note on the confinement problem. *Commun. ACM*, 16(10):613–615, October 1973.

[LT06] Michael D. LeMay and Jack Tan. Acoustic Surveillance of Physically Unmodified PCs. In *Proceedings of the 2006 International Conference on Security & Management*, June 2006.

[LvW08] G. Leus and P. van Walree. Multiband OFDM for Covert Acoustic Communications. *IEEE J.Sel. A. Commun.*, 26(9):1662–1673, December 2008.

[MSTS05] Anil Madhavapeddy, David Scott, Alastair Tse, and Richard Sharp. Audio Networking: The Forgotten Wireless Technology. *IEEE Pervasive Computing*, 4(3):55–60, July 2005.

[MTZ10] K. McCoy, B. Tomasi, and G. Zappa. JANUS: the genesis, propagation and use of an underwater standard. In *European Conference on Underwater Acoustics*, July 2010.

[NCPV13] Rajalakshmi Nandakumar, Krishna Kant Chintalapudi, Venkat Padmanabhan, and Ramarathnam Venkatesan. Dhwani: secure peer-to-peer acoustic NFC. In *Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM*, SIGCOMM '13, pages 63–74, New York, NY, USA, August 2013. ACM.

[NG12] Ivor Nissen and Michael Goetz. Generic UnderWater Application Language (GUWAL) - Specification of Tactical Instant Messaging in Underwater Networks. Technical Report WTD71 - 0070/2012 FR, Research Department for Underwater Acoustics and Marine Geophysics, Kiel, Germany, December 2012.

[OAC+12] R. Otnes, A. Asterjadhi, P. Casari, M. Goetz, T. Husøy, I. Nissen, K. Rimstad, P. van Walree, and M. Zorzi. *Underwater Acoustic Networking Techniques*. SpringerBriefs in Electrical and Computer Engineering. Springer, 2012.

[ON10] Ramanagouda Odugoudar and Ivor Nissen. Ad-hoc Network Emulation Framework for Underwater Communication Applications. In *Proc. 5th ACM International Conference on Underwater Networks & Systems*, Woods Hole, MA, September 2010. ACM.

[Owa13] Nancy Owano. Authors explore security threat of covert acoustical mesh networks in air. `http://phys.org/news/2013-12-authors-explore-threat-covert-acoustical.html`, Accessed: 2013-12-02, December 2013.

[PK00] Natalie Packham and Frank Kurth. Transport of context-based information in digital audio data. In *Audio Engineering Society 109th Convention*, September 2000.

[Roh] Rohde & Schwarz. R&S PR100 Portable Receiver On-site radiomonitoring from 9 kHz to 7.5 GHz. `http://www.rohde-schwarz.de/file/PR100_bro_en.pdf`, Accessed: 2013-12-02.

[TOD+10] David Tofsted, Sean O'Brien, Sean D'Arcy, Edward Creegan, and Scott Elliott. An Examination of the Feasibility of Ultrasonic Communications Links. Technical Report ARL-TR-5200, Army Research Laboratory, White Sands Missile Range, NM, USA, June 2010.

[vWLS+09] Paul van Walree, Thorsten Ludwig, Connie Solberg, Erland Sangfelt, Arto Laine, Giacomo Bertolotto, and Anders Ishøy. UUV Covert Acoustic Communications. In *Proceedings of the 3rd conference on Underwater Acoustic Measurements: Technologies and Results*, June 2009.